STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

EFFECTS OF INFORMATION OPERATIONS ON NONLINEAR FORCE STRUCTURES

BY

LIEUTENANT COLONEL SUSAN S. LAWRENCE
United States Army

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 4

19990521 022

USAWC STRATEGY RESEARCH PROJECT

EFFECTS OF INFORMATION OPERATIONS ON NONLINEAR FORCE STRUCTURES

by

LTC Susan S. Lawrence
United States Army, Signal Corps

Colonel Michael A. Pearson
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: LTC Susan S. Lawrence

TITLE: Effects of Information Operations on Nonlinear Force Structures

FORMAT: Strategy Research Project

DATE: 20 March 1999 PAGES: 37 CLASSIFICATION: Unclassified

This paper will address the advent of information operations and its effect on how the military will operate in the future. The goal is to highlight the need to aggressively pursue the execution of information operations' strategy and doctrine. Wrapped in this is the requirement to fix responsibility, clarify terms and understanding of IO, and find creative ways of responding to this new order of business. This may mean a whole new way of thinking that may alter our force structure to be more responsive to a threat.

This paper also introduces the theory of nonlinearity and its effect on information operations. Leadership, innovation, and flexibility of task organization are essential to the success in Army operations. Future force designers must look at each mission uniquely and apply the right size and type of forces to meet the threat. This means units deploying in non-traditional ways; thus, the challenge of providing smooth, reliable information operations.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

"We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

- Joint Vision 2010[1]

. . . thus the birth of information operations and warfare. Most readers of this quote will agree with it in principle. Most will agree we are entering a new age, the information age and that the current technology revolution effects us personally and professionally. All one has to do is pick up the paper and see the next horror story about Y2K. Most would say information operations (IO) and information warfare (IW) are critical to future world dominance. This paper will address the advent of information operations and warfare and its effect on how the military will operate in the future.

The goal is to highlight the need to aggressively pursue the execution of information operations' strategy and doctrine. Wrapped in this is the requirement to fix responsibility, clarify terms, and find creative ways of responding to this new order of business. This may mean a whole new way of thinking that may alter our force structure to be more responsive to a threat. The ultimate end is to ensure the commander has

accurate battlefield situational awareness, while at the same time disrupting the enemy's decision cycle.

Critical to the success of information operations is the sharing and protection of needed information. In a sterile, linear world of information operations, the flow of information goes from Department of Defense, to an Army representative, to corps, to division, to brigade. Each of these units operates from somewhat the same Standing Operating Procedures. They train with each other and know what to expect from each other. Today, the United States Army operates at an extremely high pace with the increased frequency of peacekeeping missions; i.e. Restore Hope, Uphold Democracy, Operation Joint Guard and now Operation Southern Watch. Leadership, innovation, and flexibility of task organization are essential to the success in Army operations.

Many of the deployments have found units in a country with little to no communication infrastructure. Couple this with no support from the normal higher Corps headquarters and the challenge of nonlinearity for information operations is complicated. This was the case in Operation Desert Thunder/Operation Southern Watch. General Anthony Zinni, Commander in Chief, United States Central Command (CINC, USCENTCOM), task organized a response task force to meet the challenge from Iraq when they violated the peace agreement and

failed to cooperate with the UNSCOM inspectors. General Zinni pulled forces from 3d Infantry Division (Mechanized), 101st Airborne Division, 82d Airborne Division plus additional joint assets and consolidated this land-based force under a single Coalition Task Force Commander. His goal was to take "just enough, just in time" to respond to the threat. The Army did not need, nor can we continue to afford, to build up a force the size used in Operation Desert Shield/Desert Storm.

By deploying in this manner, units were organized in non-habitual and in a non-traditional fashion. Lieutenant General Richard A Chilcoat states, ". . . I am convinced that the ability to thrive in nonlinear environments will have to be among the core competencies of the warrior and statesman of the 21st century if the United States is to maintain its position."[2]

The United States Army is entering an extremely challenging, exciting future as it addresses the issues of fielding new technology and finding unique answers to aligning the right size and type of force against a defined mission. How does it adequately introduce a new combat multiplier known as information operations and information warfare while at the same time operating in a nonlinear world of multiple military operations other than war?

The goal of this paper is to describe the current policy on information operations (Sections 1 - 3). Included in this

discussion is an analysis of the policy and its adequacy projected out to 2010 using the ends-ways-means model introduced by Colonel (Ret) Lykke[3]. Additionally, the paper will identify a few alternative approaches to the current policy. Section 4 describes what type of information is included in information operations and why it is critical to the commander on the ground. Section 5 expands on the complexity of the nonlinear challenge and how it effects the information described in Section 4. Section 6 will discuss the threat to information operations and how it effects the Warfighters. The paper ends with a conclusion and a few informed recommendations. One must first articulate the current national security strategy to fully understand the role of information operations and how it will play in future nonlinear military affairs.

SECTION 1 - CURRENT STRATEGY ON INFORMATION OPERATIONS

> ***Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting or denying an adversary's ability to do the same. While it is depended upon superior technology, systems integration, organization and doctrine, it is not an inherent quality but, like air superiority, must be achieved in the battlespace through offensive and defensive information operations.***[4]

The current national security strategy for information operations is the means to sustain continuous military operations that enable, enhance and protect the friendly force's ability to collect, process, and act on information and to

achieve an advantage across the full range of military operations. At the same time, information operations include exploiting or denying an adversary to collect the same information.[5] This strategy includes military operations at all levels; strategic, operational, and tactical. Information operations become information warfare when IO is conducted during a time of crisis or conflict.

Why is there a need for a national security strategy on information operations? Alvin and Heidi Toffler may best describe the evolution, or some may say revolution, to the information technology age. In their books *The Third Wave* and *War and Anti-War*, the Tofflers describe historical epochs characterized by revolutionary and technological breakthroughs that cause waves of socioeconomic change. The first wave is known as agrarian. Animal domestication and agricultural cultivation characterize it. The second wave is industrial. Mechanization, mass production and the division of labor characterize this wave. The authors profess we are now entering a third wave - information. An age characterized by digitization, computers and information technologies.[6]

The Department of Defense published two documents to give commanders and staff some guidelines in defining the scope of the military's responsibilities in the area of information operations. Those two documents are Department of Defense

Directive S-3600.1, Information Operations, and Chairman of the Joint Chiefs of Staff Instruction 3210.01A, Joint Information Operations Policy. Do these guidelines and the current information operations strategy posture us well into the 21st Century? The following section identifies the ends associated with the strategy of information operations and the ways and means to accomplish those ends.

SECTION 2 - ANALYSIS OF EXISTING STRATEGY

"History does not teach that better technology necessarily leads to victory. Rather victory goes to the commander who uses technology better, or can deny the enemy his technology."

- Office of the Chief of Naval Operations[7]

The Report of the Quadrennial Defense Review, May 1997, lists information operations as a critical enabler; critical to our nation's power projection. The future communication networks and systems must allow for timely exchange of information, data, decisions and orders. Simultaneously, defensive information operations must deny the enemy's ability to interfere in friendly information operations.[8]

The "end" or objective, using Lykke's model, is for the United States to have information superiority over our adversaries. Information dominance gives a tremendous strategic and military advantage. Will current ways and means support the continuation of information superiority into 2010?

There are multiple activities ongoing to provide the "ways" to gain information dominance. In March 1996, Attorney General Janet Reno asked several cabinet members to create a Cyberspace defense "entity" to help establish a national Cyberwar defense policy given the proliferation of information operations.[9] This is one of many current activities in an effort to counter what intelligence and defense officials say is a new national security threat.

The Defense Science Board is heading another effort entitled Information Warfare - Defense. It is this board's conclusion that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States. Such an attack would seriously effect the ability of the Department of Defense to carry out its assigned missions and functions.[10]

TF XXI is a huge commitment towards the understanding of offensive and defensive information operations. One critical lesson learned in recent testing is the need for soldiers who understand and can operate information systems from end to end. Another crucial lesson learned indicates a continuing problem with interference and lack of available frequencies. More resources (means) must be dedicated to further enhancing communication grids.

On 20 May 1998, Brigadier General William L. Bond, Army Digitization Office, briefed these lessons plus many others. At the conclusion of the briefing, BG Bond stated the current investment strategy puts the priority on information dominance.[11] Advancements in information operations will continue if there is a commitment to these "means", i.e. the investment strategy. The Department of Defense must meet the 21st Century postured to exploit technology, coupled with training, to develop information operations. This will give the United States the undeniable qualitative advantage over our adversaries.

Only a few of many ongoing initiatives on the strategy of information operations is covered in the scope of this paper. Following is a summary using Lykke's ends-ways-means model on strategy for information operations:

ENDS	WAYS	MEANS
National Objectives	National Concepts	National Resources
• Information Dominance	• National Defense Science Board • Executive Order 13010 • Cyberwar Defense Policy	• Funding • Education • R&D •Experimentation (TF XXI) • Army After Next

Figure 1. Use of Lykke Model

One of the five principal components of the evolving Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture for 2010 and beyond is that information operations must be capable of penetrating, manipulating or denying an adversary's battlespace awareness or unimpeded use of his own force.[12] Fifteen years from now, our forces need to see the battlespace deeper. Battlefield situational awareness is key to the commander making timely decisions and taking the initiative away from the enemy. This is critical to the success of information operations and ultimately information warfare during conflict. How can we better focus ways and means to ensure information operation success in the future?

SECTION 3 - ALTERNATIVE APPROACHES

"There is a war out there, and it's all about who controls the information. It's all about the information."

- Cosmo in Sneakers[13]

Secretary of Defense, William S. Cohen, states in the Quadrennial Defense Review he believes the United States is well on its way in its efforts to exploit information technology to transform the U.S. military. The primary efforts and resources are placed in the area of protecting critical United States infrastructure against hostile information operations. Development continues in U.S. information operations

capabilities for use in peacetime activities, smaller-scale contingencies, and major theater wars.[14]

On the other hand, the National Defense Panel, 1997, is rightfully concerned about where information technology is going. The panel stated information technology is a two-edged sword of both tremendous opportunities and vulnerabilities.[15] Vulnerabilities range from disruption of communication networks to small-time hackers to all out terrorism against critical information networks. Future leaders must heed the concerns of these vulnerabilities. This discussion will be expanded in a follow-on section. On a positive note, General Hugh Shelton, Chairman, Joint Chiefs of Staff has made Information Operations one of his top six priorities.[16]

There are multiple avenues to explore as we review the national security strategy and the execution of information operations. Unstated, but obvious is the need to understand the realm of information operations planning, coordinating, integrating and deconflicting joint IO.

Second, is the alternative approach that information operations are considered another combat multiplier and weapon. We can strike lethally with planes, tanks, and artillery. The same is true with offensive information operations. If friendly forces can disrupt enemy lines of communication, uncover

critical intelligence sources and alter their global positioning equipment through Cyberspace, we will deliver a decisive blow.

A third alternative approach is the role of Cyberspace. This is the worldwide interconnection of communications networks, computers, and databases that make vast amounts of information available. This concept is also termed global information infrastructure.[17]

Fourth, is to combine all current initiatives related to information operations into a single agency. Currently, each service, the Department of Intelligence Agency (DIA), Office of the Secretary of Defense (OSD), and J6, Joint Chiefs of Staff (JCS), have committed resources to exploring information operations. The Department of Defense needs to incorporate efforts to reduce duplication and define a single strategy for information operations. This will also eliminate the confusion of multiple definitions and terms associated with information operations. Dissemination of defined strategy and doctrine will help tremendously in understanding the role and context of information operations.

Before this paper discusses the complexity of nonlinearity on information operations, what information does the commander need on the battlefield to win and how is this information fused for defensive and offensive operations?

SECTION 4 - REQUIRED INFORMATION

Today, many different organizations are defining information operations in somewhat different terms, but the theme of what information is included within information operations is standard. A brief discussion of these categories follows.

SECURE COMMUNICATIONS WITH HIGHER HEADQUARTERS

First and foremost, a commander requires secure voice and data communications with all headquarters, higher, lower and laterally. These links may take many forms; GCCS, SIPRNET, and tactical telephones just to name a few. Orders, mission guidance, commander's intent, PIRs, CCIRs, logistical data, force flow and situational updates must be readably available to all command headquarters. It is essential that this information be passed quickly and accurately. This will shorten the commander's decision making cycle, giving him a tactical advantage over the enemy.

SECURE COMMUNICATIONS WITH JOINT AND ALLIED FORCES

In order to effectively command and control the total force, a commander must have secure data communications when deployed with joint and combined forces. On today's battlefield, the primary means of transmitting orders, spot reports, and combat updates is some form of voice communications; i.e. FM. A faster and more reliable means is

data communications. Any system used by the forces must be capable of interfacing with all coalition forces. In addition to using NIPRNET and SIPRNET over MSE, the use of Video Teleconferencing (VTC) has greatly increased.

VTC provides commanders simultaneous, multi-point, real time, voice and video connectivity. This means allows a commander to more clearly convey his intent through the use of real time voice and simultaneous display and graphical data. For example, a commander can conduct a rehearsal of a plan with subordinate and allied commanders and staffs in their own Tactical Operation Centers.

INTELLIGENCE RESOURCES

The commander must have timely and accurate answers to Commander's Critical Information Requirements (CCIR). With this, a commander is better able to visualize his battlespace and apply the correct amount of force at the critical time and place to achieve decisive victory. This requires access to real time intelligence products from a variety of sources to include national-level resources, and local open sources such as news media, commercial sources and academia. As proven in the Gulf War, the international news media is on the cutting edge of world events. The media provides pictures and first hand data, many times faster then a conventional intelligence channel receives, processes, analyzes, and disseminates information.

The commander also needs real-time targeting information through national reconnaissance, intelligence, surveillance and target acquisition (RISTA) assets.

The intelligence effort provides current, accurate threat and targeting data to weapon systems and intelligence sensors. Their effectiveness is dependent upon the rapid movement of data between collector, processor, decision-maker, and shooter.

-- FM 100-6[18]

RESPONSIVE LOGISTICS SYSTEM

Joint Force Commanders need to establish and coordinate a flexible and responsive logistical support system. A responsive supply system provides the commander flexibility to exploit opportunities on the battlefield. They supply system must respond to the commander's intent and his priorities while anticipating future requirements. Accurate and timely information is a must. Data communications play an integral part in flowing supplies into a theater, especially since the supply systems transitioned from a mass system into a just enough, just in time support system. Modern sophisticated military logistics requires reliable communication systems. Just enough, just in time supply system relies both on robust data communications and a dependable transportation network.

SPLIT BASE CAPABILITY

A deployed commander must leverage existing Army and Department of Defense (DOD) agencies for split base operations.

As we have seen in the past, a division rarely deploys in its entirety. Forward force packaging results in only a portion of the division being forward deployed with the remainder in the division base. Therefore, to conduct split base operations, a commander must have access to both classified and unclassified voice and data communications with home station and DOD agencies. Specifically, but not conclusively, a commander needs to access DSN, SIPRNET, NIPRNET, and VTC.

MORALE SUPPORT OPERATIONS

Rear Detachment operations and Family Support Group activities have evolved since Operation Desert Storm. The ability for a soldier to maintain communications with home station increases morale and is a combat multiplier. Additionally, these operations are a commitment to our high quality soldiers. Through these communication channels, the soldier can update his records and prepare for promotion boards. Support tools available to the commander are electronic mail (E-mail) and morale support telephone calls. Electronic mail supplements postal operations and can provide rapid communications even in the early states of a deployment when postal operations are still being coordinated. Limited morale support telephone calls through a tactical switch can reassure family members and provide the soldier peace of mind.

The above generic fields are critical information needs to the commander if he is to win the information operations battle. There are many more including PSYOPS activities, civil affair, PAO, etc. FM 100-6 (Information Operations) reiterates "A commander's battlespace now includes global information connectivity. As a result, tactical military actions can have political and social implications that commanders must consider as they plan, prepare for, and conduct operations. "Know the situation" now requires additional focus on nonmilitary factors. Commanders can best leverage the effects of new technology on their organizations by employing new and emerging automated planning and decision aids and new or different methods and techniques of control and management."[19]

In the past, passing information on the battlefield was linear, i.e. communications passed from higher to lower and left to right. Today's force designers now face the challenge of nonlinearity. The units on the left are in all likelihood coalition partners. The division's higher headquarters will probably not be the normal affiliated corps. Czerwinski's studies identify:

> *The connotations of nonlinearity are a mix of threat and opportunity. Nonlinearity can generate instabilities, discontinuities, synergisms and unpredictability. But it also places a premium on flexibility, adaptability, dynamic change, innovation and responsiveness . . .*[20]

Let's now apply this nonlinear challenge and examine its affect on information operations.

SECTION 5 – THE NONLINEAR CHALLENGE

> ***"The architects of the US Army's future face an experience which in many ways parallels that of a century ago. Today's force designers, like those at the last turn of the century, must wade through a sea of futuristic materials, some fantastic, some prescient, to make projections about the future geopolitical environments and military-technological capabilities."***
>
> ***– Antulio J. Echevarria II***[21]

Providing uninterrupted flow of information on the battlefield is critical to information operations. What is the concept of nonlinearity and why does it complicate information operations? The American Heritage College Dictionary defines nonlinear as "not in a straight line".[22] Therefore, nonlinear is the concept of anything that strays from the straight and normal way of operation. A number of articles and books are now appearing on this subject. A few examples are Douglas A. Macgregor's "Breaking the Phalanx: A New Design for Landpower in the 21st Century", Tom Czerwinski's "Coping with the Bounds, Speculation on Nonlinearity in Military Affairs", and Alan Beyerchen's "Clausewitz, Nonlinearity and the Unpredictability of War". Of keen interest is Czerwinski's analysis, "In fact, Clausewitz is the emblem of nonlinearity in military affairs.

It is said that Clausewitz is more often quoted than read. The reason is simply that he is hard to read linearly."[23]

Linearity in and of itself was challenged during Operation Desert Thunder 1998. CENTCOM and 3d Army were the clear, defined strategic leaders of Operation Desert Thunder and served as the Headquarters, Coalition Task Force (CTF). The 3d Infantry Division (Mechanized) deployed as the tactical unit. The challenge for information operations came when XVIII Airborne Corps did not participate in the operation. The habitual and linear relationship between XVIII Airborne Corps to the 3d Infantry Division (Mechanized) vanished. The division faced a non-traditional relationship and there were multiple challenges to information operations. The task from CENTCOM to 3d ID (M) was to deploy with just enough, just in time with the right assets to execute an offensive operation against the threat of Iraq.

Specifically, the 123d Signal Battalion was tasked to provide communication support to the 3d Infantry Division (Mechanized) mission for Operation Desert Thunder. The original guidance was for one company's worth of node centers and just enough additional equipment to support a division tactical command post, division jump command post, 1 brigade combat team command post, Force Field Artillery command post, aviation command post and the FST. There was also a requirement to be

prepared to provide connectivity to joint and allied forces; initially unidentified.

Based on this guidance, the battalion deployed with what was believed to be a sufficient support package. Once in country, it became very clear that the unit would need more assets to solidify the network and reachback to the CTF headquarters at Camp Doha. Permission was granted to deploy more assets early in the force flow.

Although the internal division tactical communications were adequate, communications to EAC headquarters were inadequate. Thus, the nonlinearity deployment became the challenge. This challenge will be faced again. Future force designers will confront budgetary, doctrinal, and proponency battles as they build the right task force for the right mission. Understanding of fighting with smaller size units will become more apparent as results of Force XXI and Army After Next projects are published.

This paper has so far reviewed the strategy of information operations and information warfare, coupled with the complexity of nonlinearity. The future of both new concepts faces certain threats. Threats the United States Army has not faced before. Threats from potentially new enemies.

SECTION 6 - THE THREAT

". . . a year of deception, broken codes, satellites, missile bases and the ultimate sting

operation --and how one ingenious American trapped a spy ring paid in cash and cocaine, and reporting to the KGB."

- Cliff Stoll's <u>The Cuckoo's Egg</u>[24]

The explosion of information operations on the Army's near horizon has caused a great deal of assets to be committed towards its understanding. Many governmental agencies are trying to outline what must be done to ensure information superiority. Couple this with the emergence of nonlinearity in task organizations, deployments, and unique missions and it becomes apparent the highest level of our government must get involved with defining the roadmap. The National Security Strategy for a New Century, May 1997 states,

> *The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.*[25]

Information operations and information warfare have introduced a whole new category of words that should first be understood before we proceed with the threat. Martin Libicki of

the National Defense University has written a few easy to understand definitions. They are:

- *C2 Warfare:* attacks on our ability to generate commands and communicate with the services and deployed forces
- *Electronic Warfare:* techniques that enhance, degrade, or intercept flows of electrons or information
- *Intelligence-based Warfare:* integration of sensors, emitters, and processors into reconnaissance, surveillance, target acquisition, and battlefield damage assessment systems
- *Psychological Warfare:* designed to affect the perception, intentions, and orientations of decisionmakers, commanders, and soldiers
- *Cyberwar:* the use of information systems against the virtual personas of individuals or groups
- *Hackerwarriors:* who use their techniques to destroy, degrade, exploit, or compromise information systems
- *Economic Warfare:* expressed in one of two forms: as an information blockade (which presumes that information flows are as important as supply flows) or as information imperialism (which presumes one believes that trade is war)[26]

There are more and more published articles about threats against our way of life since the introduction of information operations. First was during the middle 1980's when a group of hackers accessed the Internet through Lawrence Berkley Lab to acquire military and commercial secrets. The hackers were found in West Germany and ultimately led to a spy ring working for the KGB. These hackers accessed over 40 different military and defense computers.[27] A second renown case is in 1995 when a 28-year-old Russian biochemistry graduate student, Vladimir Levin, used computer codes more than 40 times to break into New York Citicorp's computerized system. He transferred over $12 million

to banks around the world. These two cases underscore our national vulnerability as we enter the new Information Age.

The military strategists and policymakers must explore how to protect national assets from information assaults. How can our leaders deter this threat? The National Military Strategy of the United States asserts one of our goals is to win the information war. To do this, one must first recognize the unknowns. To begin with, there is the complexity of the law and working internationally and between government, civilian, and military organizations. Today there are no international agreements. The two cases cited in this paper suggest the need for one.[28]

Another element to the threat of information operations is the psychological weapon. Today's media capability helps to manipulate perceptions, emotions, interests and choices.[29] One just needs to look back to Operation Desert Fox with CNN reporters standing on top of the building and announcing the imminent attack on Iraq. This image was immediately transmitted around the world. There were mixed perceptions, emotions, and interests, i.e. did the United States have the right to bomb Iraq, were civilians wrongfully targeted, why now, was it timed to what was happening with the impeachment trial? Rogue hackers know that mass medium can manipulate and taint sources. It is

also very easy to expand the threat by including false data into information systems.

Two final elements of threat to consider are the speed in which information assaults can happen and the availability of information to anyone.[30] The military has early warning devices for missile attacks. There is no such warning for an attack on information systems. Also, the access to information is far reaching. Any novice can access the Internet and learn how to build a bomb.

The above elements of threat are a huge challenge to our national leaders. We find ourselves facing a fast-changing way of doing business with the introduction of information operations and warfare as a new strategy and future force designers finding nonlinear solutions to operations other than war.

SECTION 7 - RECOMMENDATIONS AND CONCLUSION

"Current interests in information warfare and the manifold effects of the information revolution on the conduct of war cause many to proclaim a revolution in warfare."

- Ryan Henry and C. Edward Peartree[31]

The most critical recommendation one can make is that every member associated with the Department of Defense recognizes that

understanding information operations is a responsibility at every level of command. This area of national security strategy does not just affect the intelligence or signal corps communities. It touches every boundary of combat and peacetime operations.

Secondly, it is important we understand information systems from end to end. This entails the means of communications, data being distributed, troubleshooting and very importantly the protection of information systems. It is very plausible that by 2010 no member of the Armed Forces will carry currency. All money transactions are conducted over the Internet with one's personal bank. It is very plausible that all logistical actions are done electronically with no paperwork trail. This makes the Armed Forces very vulnerable to enemy attacks on our information systems.

Thirdly, America's leadership must pin the rose on someone. There must be a single advocate for information operations. Is it a service chief, J6, DIA, a CINC or should it fall within the realm of doctrine? No matter who, there must be a leader who will well represent IO interests in the national debate that will shape our future. This includes articulating the national interest and the ways and means.

Lastly, the ability of the force designers to think "outside the box" is critical in contributing the right assets

to the right operation. Nonlinearity is caused by the advent of technology and there must be innovative solutions. Douglas A. Macgregor presents and argues there may be a minimal need for ground forces at all in the next century.[32] This makes it critical that future leaders understand the elements of Information Operations and Information Warfare and know how best to ensure information superiority.

In closing, the National Defense Panel states that if we refuse to change in a timely manner, if we refuse to understand this new technology age we are entering, then we risk being fundamentally unprepared for the future. This puts in question the security of future generations of Americans.[33] Our leaders must adhere to this advice as we dedicate the ways and means to ensure information dominance.

Word Count - 5523

ENDNOTES

Chairman, Joint Chiefs of Staff, U.S. Joint Chiefs of Staff. Joint Vision 2010 - America's Military Preparing for Tomorrow (Washington D.C.: U.S. Government Printing Office, May 1996).

Tom Czerwinski, Coping with the Bounds, Speculations on Nonlinearity in Military Affairs, (Washington, DC: National Defense University, 1998), xiv.

U.S. Army War College, Department of National Security and Strategy. Readings on War, National Policy, and Strategy. Carlisle Barracks: 1998. VOL I. "Toward an Understanding of Military Strategy" by Arthur F. Lykke, Jr.

Chairman of the Joint Chiefs of Staff, National Military Strategy of the United States of America (Washington D.C.: U.S. Government Printing Office, 1997), 18.

[5] Headquarters, Department of the Army. FM 100-6 Information Operations. August 1996, 2-3.

Alvin and Heidi Toffler, War and Anti-War, Survival at the Dawn of the 21st Century, (New York: Little, Brown and Company, 1993), 3 - 5.

Winn Schwartau, Information Warfare (New York: Thunder's Mouth Press, 1994), 291.

Secretary of Defense, Report of the Quadrennial Defense Review, (Washington D.C.: U.S. Government Printing Office, 1997), 17.

Wendell C. Baker, Janet Reno's New Cyberwar Policy", Washington Technology, 20 April 1996.

Office of the Under Secretary of Defense for Acquisition & Technology, Report of the Defense Science Board Task Force on Information Welfare - Defense (IW-D), November 1996.

BG William L. Bond, Army Digitization Office Briefing, Military CIS 98, 20 May 1998.

Secretary of Defense, Report of the Quadrennial Defense Review, p. 39.

[13] Schwartau, 215.

[14] Secretary of Defense, 50.

[15] National Defense Panel, National Defense Panel Report (Washington D.C.: U.S. Government Printing Office, 1997), 64.

[16] MG George F. Close, J7, Briefing to the USAWC Class, 11 February 1999.

[17] Joint Chiefs of Staff, Joint Publication 3-13 (Second Draft), (Washington D.C.: U.S. Government Printing Office, 1997), GL-6.

[18] Headquarters, Department of the Army. FM 100-6 Information Operations. August 1996, 4-3.

[19] Headquarters, Department of the Army. FM 100-6 Information Operations. August 1996, 1-12.

[20] Czerwinski, 11.

[21] Antulio J. Echevarria II, Tomorrow's Army: The Challenge of Nonlinear Change, (Parameters, Autumn 1998), 85.

[22] The American Heritage College Dictionary, Third Edition, (Boston, New York: Houghton Mifflin Company, 1997), 928.

[23] Czerwinski, 3.

[24] Cliff Stoll, The Cuckoo's Egg, (New York: Pocket Books, 1990), Back Cover.

[25] President of the United States of America, A National Security Strategy for a New Century, (The White House, May 1997), 14.

[26] Timothy L. Thomas, Deterring Information Warfare: A New Strategic Challenge, (Parameters, Winter 1996-97), 83.

[27] Stoll, The Cuckoo's Egg.

[28] Timothy L. Thomas, Deterring Information Warfare: A New Strategic Challenge, (Parameters, Winter 1996-97), 84.

[29] Thomas, 85.

[30] Thomas, 86.

[31] Ryan Henry and C. Edward Peartree, Military Theory and Information Warfare, (Parameters, Autumn 1998), 121.

[32] Douglas A. Macgregor, Breaking the Phalanx: A New Design for Landpower in the 21st Century, (Westport, Connecticut, Praeger, 1997) xii.

[33] National Defense Panel, 87.

BIBLIOGRAPHY

Baker, Wendell C. Janet Reno's New Cyberwar Policy. Washington Technology, 20 April 1996.

Bond, William L. BG. Army Digitization Office Briefing. Military CIS 98, 20 May 1998.

Chairman, Joint Chiefs of Staff, U.S. Joint Chiefs of Staff. Joint Vision 2010 - America's Military Preparing for Tomorrow. Washington D.C.: U.S. Government Printing Office, 1996.

Czerwinski, Tom. Coping with the Bounds, Speculation on Nonlinearity in Military Affairs. Washington D.C.: National Defense University, January 1998.

Echevarria, Antulio J. II. Tomorrow's Army: The Challenge of Nonlinear Change. United States Army War College, Parameters, Autumn 1998.

FM 100-6. Information Operations. Headquarters, Department of the Army, Washington D.C.: U.S. Government Printing Office, August 1996.

Henry, Ryan and Peartree, C. Edward. Military Theory and Information Warfare. United States Army War College, Parameters, Autumn 1998.

King, Edward L. The Death of the Army: a Pre-Mortem. New York: Saturday Review Press, 1972.

Lykke, Arthur F., Jr. Toward an Understanding of Military Strategy. U.S. Army War College, Department of National Security and Strategy. Carlisle Barracks, 1998.

Macgregor, Douglas A. Breaking the Phalanx - A New Design for Landpower in the 21st Century. Center for Strategic and International Studies, 1997.

Office of the Under Secretary of Defense for Acquisition & Technology. Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D). Washington D.C.: U.S. Government Printing Office, November 1996.

Schwartau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1994.

Secretary of Defense. Report of the Quadrennial Defense Review. Washington D.C.: U.S. Government Printing Office, 1997.

Snyder, Frank M. Command and Control, the Literature and Commentaries. Washington D.C.: National Defense University, September 1993.

Stoll, Cliff. The Cuckoo's Egg. New York: Pocket Books, 1990.

Strawn, James C., Lieutenant Colonel, U.S. Army. Information Operations Challenges. Carlisle Barracks, PA: United States Army Warm College, March 1998.

The American Heritage College Dictionary, Third Edition. Boston, New York: Houghton Mifflin Company, 1997.

Thomas, Timothy L. Deterring Information Warfare: A New Strategic Challenge. United States Army War College: Parameters, Winter 1996-97.

Toffler, Alvin and Heidi Toffler. War and Anti-War. New York: Little Brown and Co., 1993.

U.S. Joint Chiefs of Staff. Joint Publication 3-13. Washington D.C.: U.S. Government Printing Office, 1997.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington D.C.: U.S. Government Printing Office, 1997.

U.S. National Defense Panel. National Defense Panel Report. Washington D.C.: U.S. Government Printing Office, 1997.

U.S. Office of the White House. National Security Strategy of the United States. Washington D.C.: U.S. Government Printing Office, May 1997.